UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,246	12/29/2000	Louis A. Lippincott	42390P9941	8803

8791 7590 05/26/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/753,246	LIPPINCOTT, LOUIS A.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/13/06*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20 are pending.**

2. **The amendment of 9/12/05 has been received and entered.**

Response to Amendments

3. In view of the amendments of 9/12/05, a new grounds of rejection has been issued.

Applicant's arguments however on pages 5-6, referencing Easter, column 3, line 65 – Column 4, line 10 appear to imply that because Easter et al. discloses that the array is a fusible array, hardware can therefore not be changed at regular intervals.

The Examiner disagrees with this interpretation however. Easter et al.(Abstract) explicitly discloses that a particular advantage of the invention is to allow a data processing system to be dynamically upgraded without hardware replacement.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al. US patent 5530749 and Elgamal et al., US patent 5657390.

In reference to claim 1:

Easter et al. (Column 6, lines 15- Column 7, line 23) discloses a computer product, comprising:

- first computer readable program code embodied in a computer usable medium to cause a computer to recieve a message that includes an encrypted hardware configuration code for configuring hardware and receive a key associated with an encrypted code defining a unique hardware configuration,
- where the hardware configuration code is the value Nc, and where Nc, is part of a message that is sent to the cryptographic configuration processor hardware, and therefore "received" by such hardware, and where the hardware configuration is encrypted or "encoded" with an XOR operation.(Column 6, lines 43-58) & (Column 7, lines 15-25) and a key is received by the computer through an optical disk (Column 6, lines 59-62), and the key that is received is Kp (Column 6, lines 43-58).
- second computer readable program code embodied in a computer usable medium to cause a computer to decrypt the encrypted code based upon the stored key, where the encrypted code is decrypted with the public key (Column 7, lines 15-23)
- third computer readable program code embodied in a computer usable medium to cause a computer to program a re-configurable hardware block based upon the decrypted key to establish a unique hardware configuration, where the logic array within the chip is based

upon the decrypted key used to establish the hardware configuration. (Column 3, lines 65 – Column 4, line 10)

Easter et al. fails to explicitly disclose an program code to cause a computer to perform a decryption operation on encrypted information utilizing the unique hardware configuration.

(Elgamal et al. Figure 12c) discloses a method in which a computer with a hardware configuration in a computer is used to decrypt encrypted information using the Secure Sockets Layer Protocol.

Elgamal (Column 1, lines 10-20) also teaches that there is a need for confidentiality of communications in a network transmission.

Easter et al. also fails to explicitly disclose that the configuration is changed at regular intervals. Easter et al. however does disclose that the configuration may be changed dynamically without hardware replacement. (Abstract) & (Column 1, lines 40-58) & (Column 2, lines 15-20) The Examiner notes however that upgrading the configuration dynamically can be done with only two possibilities, regularly or irregularly. More often than not changes in hardware configuration are performed regularly. (for example, a weekly hardware maintenance or an annual upgrade to a security system)

It would have been obvious to one of ordinary skill in the art at the time of invention to further use the computer whose hardware had been configured to decrypt encrypted information it received such as SSL, or other encryption/decryption operations common to web usage, in order to fulfill the need to ensure confidentiality of computer network communications and to upgrade the hardware configuration regularly so that users may know when changes in the hardware system take place to prepare for it.

In reference to claim 2:

Easter et al. (Column 4, line 60 – Column 5, line 28) & (Column 4, lines 3-23) & (Column 6, lines 59-62) discloses the computer product claimed in claim 1, further comprising:

- fifth computer readable program code embodied in a computer usable medium to cause a computer to route encrypted information through a peripheral device to the logic array, where the logic array is where the data on the module is stored (Column 4, lines 3-23), and where information from the peripheral device, the CD-ROM or the disk drive is loaded, and where the information that is loaded includes the encrypted signed configuration signature. (Column 6, lines 59-62)

In reference to claim 3:

Easter et al. (Column 4, line 60 – Column 5, line 28) discloses the computer product claimed in claim 1, further comprising:

- fifth computer readable program code embodied in a computer usable medium to cause a computer to route the incoming information through a memory interface to the logic

array, where the incoming information passes from a memory interface, the interface for the CD-ROM or disk which contains the key, to the module where the data is stored in the logic array.

In reference to claim 4:

Easter et al. (Column 4, lines 2-23) discloses the computer product claimed in claim 1, wherein the logic array includes a programmable an array of gates, where the logic array is a fusible set of wires available to logic at the other end.

In reference to claim 5:

Easter et al. (Column 4, line 60 – Column 5, line 8) discloses an electronic system comprising:

- at least one peripheral device, where the peripheral device is a CD-ROM, or a floppy disk drive which can read the flopping disk.
- a memory for storing a key associated with incoming information; and, where the floppy disk is an example of memory used for storing the key associated with incoming information, where the incoming information is the hardware configuration data.
- a chipset in communication with the at least one peripheral device, the chipset including circuitry to receive a message that includes an encrypted hardware configuration code for configuring hardware, program a reconfigurable hardware block based upon the key associated with the incoming information to establish a unique hardware configuration wherein the configuration is changed at regular intervals, where the chipset in communication with the peripheral device is the module in communication with a CD-

ROM drive or disk drive to read the key, where this information is later used program an array of gates based on that key. (Column 6, lines 25-31), and where the key is sent out to be received by the cryptographic configuration processor hardware and its circuitry therein. (Column 6, lines 43-57)

Easter et al. fails to explicitly disclose a method comprising decrypting the incoming information based on the programmed array of gates and circuitry to perform a decryption operation on the incoming information based on the configured array of gates.

However, since the configuration data is ultimately used to configure a computer, it would have been obvious to one of ordinary skill in the art to use the hardware configured computer to decrypt encrypted transmissions that it received such as SSL, or other encryption/decryption operations common to web usage, in order to allow any network transactions that involved encryption and decryption and to upgrade the hardware configuration regularly so that users may know when changes in the hardware system take place to prepare for it.

Easter et al. also fails to explicitly disclose that the configuration is changed at regular intervals. Easter et al. however does disclose that the configuration may be changed dynamically without hardware replacement. (Abstract) & (Column 1, lines 40-58) & (Column 2, lines 15-20) The

Examiner notes however that upgrading the configuration dynamically can be done with only two possibilities, regularly or irregularly. More often than not changes in hardware configuration are performed regularly. (for example, a weekly hardware maintenance or an annual upgrade to a security system)

In reference to claim 6:

Easter et al. (Column 4, lines 60 – Column 5, line 35) discloses the electronic system claimed in claim 5, further comprising:

circuitry for routing the incoming information from a peripheral device through the configured array of gates, where the key from the peripheral device(the disk or CD-ROM drive) is loaded into the module compared with the data on the configured array of gates.

In reference to claim 7:

Easter et al. (Column 4, lines 60 – Column 5, line 35) discloses the electronic system claimed in claim 5, further comprising circuitry for routing the incoming information from a memory device, the disk or CD-ROM through the configured array of gates, where the key from the memory device(the disk or CD-ROM) is loaded into the module compared with the data on the configured array of gates.

In reference to claim 8:

Easter et al. (Column 5, lines 20-25) discloses the electronic system claimed in claim 5, wherein the memory is a non-volatile memory, where the nonvolatile memory is a ROM or diskette.

In reference to claim 9:

Easter et al. (Column 6, lines 15-50) discloses the electronic system claimed in claim 5, wherein the key is a public key, where the public key is Kp.

In reference to claim 10:

Easter et al. (Column 6, lines 15-50) discloses the electronic system claimed in claim 8, wherein the key is a non-public key, where the non-public key is Ks.

Claims 11 –17 are rejected for the same reasons as claims 1-7.

In reference to claim 18:

Easter et al. (Column 4, lines 3-23) discloses the method claimed in claim 15, wherein programming an array of gates based upon the key(column 6, lines 28-32) associated with the incoming information further comprises:

programming the array of gates to provide for a unique hardware configuration upon command, where the programmed array of gates contains the data which will provide for the unique hardware configuration (Column 5, lines 4-7), and where the programmed array of gates is also in itself a unique hardware configuration. (Column 4, lines 8-10)

In reference to claim 19:

Easter et al. (Column 5, lines 20-25) discloses the method claimed in claim 15, wherein programming an array of gates based upon the key associated with the incoming information further comprises:

receiving instructions from a processor, where receiving the key to be programmed may also be received from a "service processor".

Claim 20 is rejected for the same reasons as claim 8.

Conclusion

6. The following art not relied upon is made of record:

- US patent 5355490 discloses a method of saving states of advanced processor modes
- US patent 5623604 discloses a method of remotely altering firmware
- US patent 4561059 discloses a microprocessor controlled welding apparatus

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR

1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571)272-6962.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

May 20th, 2006